IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	4:11CR3029
	)	
v.	)	
	)	FINDINGS, RECOMMENDATION
JEROD J. OLIVERIUS,	)	AND ORDER
	)	
Defendant.	)	

On February 2, 2011, Lincoln Police Investigator Corey Weinmaster prepared and submitted a warrant application to search defendant's residence at 715 West S Street, Lincoln, Lancaster County, Nebraska. County Court Judge James A. Foster issued the requested warrant; and Lincoln Police officers executed the warrant on February 7, 2011. The defendant now moves to suppress all evidence seized during the search. (Filing No. 14).

The defendant claims the evidence found during the search must be suppressed because:

1) The warrant application lacks sufficient information to support a finding of probable cause;

2) Law enforcement officers used a laptop, wireless card, and an unsecured wireless internet account to unlawfully gain access to defendant's computer files from a neighborhood street location, and absent the information obtained from this unlawful search, the warrant application failed to support a finding of probable cause.

3) The warrant was invalid because the application was vague, confusing, and misleading in describing how an unsecured wireless internet account was used to search defendant's computer.

The warrant application and warrant were filed for the court's review. (Filing No. 16). In addition, the defendant filed a copy of the affiant officer's supplemental investigation

report for the court's consideration. (Filing No. 21-1). After reviewing these documents, and for the reasons stated below, the defendant's motion to suppress should be denied without a hearing.

STATEMENT OF FACTS

The affiant officer, Corey Weinmaster, is an Investigator for the Lincoln, Nebraska Police Department, and has been a Certified Law Enforcement Officer since 1991. As set forth in detail in the warrant affidavit, Investigator Weinmaster has extensive experience and training in forensic computer examinations and computer crime investigations, including the use of peer-to-peer (P2P) file-sharing networks to commit computer crimes. Based on this training and experience, Investigator Weinmaster's warrant affidavit explains:

- Computer users can chose to install publicly available P2P software which facilitates the trading of digital files between computer users.

- P2P software connects a computer user, a "peer," to a computer designated by the software to serve as an index server, (an "ultra-peer"). Ultra-peer computers, in turn, connect with other ultra-peer computers to share index lists of available files.

- A peer can search for digital files by submitting text containing search terms to the ultra-peer. The ultra-peer searches its own files for the terms, and also sends the search terms to other ultra-peers which, in turn, examine their index list of files. If files responsive to the search are located, the requesting peer receives information from the ultra-peer on how to connect to peers with files available for sharing. The requesting peer can then choose to download files

directly from other peers, and can choose to receive the responsive files from only one source or several. Provided several files were, at one time, all part of one original file, by selecting numerous sources, the requesting peer can obtain a complete original. The P2P software will balance the network load, accept pieces of the original file from different users, and reassemble the file at the peer's local computer.

- In accordance with developments implemented by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA), digital files are assigned a Secure Hash Algorithm Version 1 (SHA1) compressed digital representation resulting in a digital signature assigned to each file. By comparing these signatures, law enforcement officers can determine if two files are, or are not, identical with a precision that exceeds 99.9999 percent certainty even if file names have been changed. The use of SHA1 compressed digital representations to match movies and images is extremely reliable.

- Peer users attempting to trade files on a P2P file-sharing network can place files from their local computer in a shared file directory, and if the peer starts the P2P software, the local computer calculates the SHA1 signature for each shared file and provides the information to other users wishing to trade files.

- Law enforcement agencies have compiled a list of SHA1 digital signatures for many child pornography images, and they use this information to conduct undercover operations involving images, video, or text files of child pornography being traded on P2P networks. When conducting this type of investigation, law enforcement officers enter search terms in the P2P software,

and receive a list of SHA1 digital signatures of responsive images available for download. If a digital signature corresponds to a file known to contain child pornography, the officer submits a download request for the file.

- Internet computers identify each other by an Internet Protocol or IP address which can, in turn, assist law enforcement officers to find the computer's internet service provider (ISP). Using the date and time the IP address was used, law enforcement can then obtain information from the service provider which identifies the account holder by name and the physical address associated with that account holder.

- By examining a list of IP addresses, law enforcement officers can locate computers reportedly in Nebraska. By comparing SHA1 digital signatures to IP addresses, they can determine whether a computer with P2P software originating from an IP address in Nebraska contains images of child pornography. Using this information, the internet service provider can identify the specific physical address of the computer.

- During an undercover internet investigation conducted by Lincoln Police Sergeant John Donahue, IP address 76.84.249.75 was identified as having files that may contain child pornography available for sharing. Regarding IP address 76.84.249.75, over 170 instances of file-sharing by the automated software occurred between March 17, 2008, and the date of the warrant application, February 2, 2011. In response to an administrative subpoena, Time Warner/Roadrunner identified the account holder for the IP address as Patrick Gilson, 715 West S Street, Lincoln, NE 68528-1419. On December

30, 2010, Sergeant Donahue was advised that this account was still using the 76.84.249.75 IP address.

- On February 1, 2011, Investigator Weinmaster parked his vehicle on the street just west of 715 West S Street, Lincoln, Lancaster County, Nebraska, and using a laptop computer with a wireless card, found 11 wireless access points, two of which provided unsecured access (no password required) with weak signals. Using the laptop and wireless card, Investigator Weinmaster noted over 90 files advertised as available from the computer at IP address 76.84.249.75, including files with the following filenames:

  13 little girl kiddy child ddoggprn lolita in(illegal_preteen_underage _ lolita_ kiddy_ child_incest_ xxx_porno_ gay_fuck_young_naked_ nude_little– girl_cum_face_ teenage_ cheerleaders_a.mpg

  PTHC (illegal_preteen_underage_lolita_kiddy_incest_little–girl_ rape_ anal_cum_ sex_lesb(1.mpg

  14 SICK (pthc) pedofilia part4 (1).mpg - Incesto vicky 2.mpg - pedofilia part4 - Vicky anal Defloration.mpg

  꽃봉 ♥ Mom & Kids - 10Yo Boy & 12Yo Girl(Pthc Pedo)-46.3.mpg

- By cross-referencing the SHA1 signatures of these files with the SHA1 signatures in the law enforcement SHA1 database, Investigator Weinmaster confirmed the four files were previously identified by law enforcement as containing child pornography. For each of the four suspect files, Investigator Weinmaster viewed a file marked with that particular SHA1 signature and confirmed the file included images of child pornography. The warrant

application includes the officer's description of the graphic images depicted in each of these four files.

The warrant application requested authority to search the premises at 715 West S Street, Lincoln, Lancaster County, Nebraska for evidence indicative of the crime of possessing and distributing of child pornography, including paper or digital files of such images, computers and computer-related information within the home, and evidence of ownership. A county court judge issued the warrant.

LEGAL ANALYSIS

A search warrant is valid under the Fourth Amendment if it is supported by probable cause. U.S. v. Stevens, 530 F.3d 714, 718 (8th Cir. 2008). When presented with a warrant application, the court must conduct a "'practical, common-sense inquiry,' consider 'the totality of the circumstances set forth,' and determine if, based on the information in the application, there exists a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" Stevens, 530 F.3d at 718 (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

Investigator Weinmaster's warrant application describes his training and experience with computer crime investigations, describes the origin of SHA1 values, and explains how law enforcement officers use these values to create a master list and database of digital images known to depict child pornography. An affiant's training and experience in child pornography investigations must be considered when evaluating the sufficiency of a search warrant application. U.S. v. Mutschelknaus, 592 F.3d 826, 829 (8th Cir. 2010).

Based on his experience and training, Investigator Weinmaster's affidavit explains that SHA1 values are 99.9999% reliable in identifying illegal pornographic images, and therefore the SHA1 assigned to an image is highly accurate and useful to law enforcement when investigating child pornography. See, e.g., U.S. v. Finley, 612 F.3d 998, 1000 n. 3 (8th Cir. 2010)("The SHA is a mathematical algorithm that allows for unique identification of digital images and videos. SHA values are, in essence, unique digital fingerprints or signatures."). The warrant application lists the names of four suspect images which were available for sharing from the computer at IP address 76.84.249.75, and this IP address was identified to a person located at defendant's residence. The names of the four listed images were highly indicative of child pornography. See U.S. v. Stults, 575 F.3d 834, 838 (8th Cir. 2009)("PTHC" stands for "preteen hard core," a term associated with images of child pornography); U.S. v. Buesing, 615 F.3d 971, 973 (8th Cir. 2010)(search terms, such as "Lolita," "pthc" ("preteen hardcore"), and "preteen," were used by the officer to locate sources of pictures and movies available through P2P sharing and depicting pornographic images of girls under the age of 18). In addition, the warrant application states that after cross-referencing the SHA1 signatures available from IP address 76.84.249.75 with those in the SHA1 database, four files were identified as depicting child pornography. The warrant application listed, by SHA1 signature, these four specific files and for each of these files, provided a description of the sex acts involving children depicted in the file.

Based on the information in the warrant application, it is unclear whether Investigator Weinmaster looked at the actual content of files retrieved from the defendant's computer to determine whether they depicted child pornography. However, contrary to the defendant's argument, even absent looking at the files within the defendant's computer and available for sharing from IP address 76.84.249.75, based on the totality of information presented in the warrant application, there was a fair probability that evidence of a child pornography crime would be found by searching the residence of the account holder for IP address 76.84.249.75.

Specifically, law enforcement officers traced IP address 76.84.249.75 to an account holder at the defendant's residence; from that IP address, officers located P2P shared files with titles highly indicative of child pornography; Investigator Weinmaster cross-referenced, by SHA1 signature, files available for sharing from IP address 76.84.249.75 with the SHA1 signatures of files known to depict child pornography; and the officer viewed four files with SHA1 signatures corresponding to those identified as containing child pornography by the SHA1 database; he confirmed the files contained graphic images of child pornography; and the application contains a graphic description of what the officer saw. Given the accuracy and reliability of SHA1 signatures and the development of a database listing of SHA1 signatures for files containing child pornography, a judge may find, in all likelihood, that a suspect's computer contains images of child pornography even if the affiant officer has not opened and viewed the files on (and using) the defendant's computer, and has not viewed files downloaded directly from that computer. U.S. v. Beatty, 2011 WL 2728298, 1 (3d Cir. July 14, 2011)(finding a sufficient showing of probable cause where officer did not open and view the suspect files, but explained the file retrieval process, provided the names of suspect files, and cross referenced and matched each file's SHA1 to known child pornography files); U.S. v. Miknevich, 638 F.3d 178, 184 (3d Cir. 2011)(holding that although the investigating officer never viewed the alleged images of child pornography on the defendant's computer, the warrant application provided sufficient probable cause where the highly descriptive names of the file contents indicated child pornography and the SHA1 values for these files matched SHA1 values of files known to contain child pornography).

As an alternative argument, the defendant claims that if Investigator Weinstein viewed files located on the defendant's computer, either directly or by download from that computer, this access to the defendant's computer was an illegal warrantless search, the results of which cannot be used as support for issuing a search warrant. The defendant argues:

> Weinmaster conducted a warrantless search when he invaded the privacy of a computer by conducting a search through an unsecured wireless access point. At the time Weinmaster accessed the computer, he was without a warrant to conduct a search. Yet he invaded the privacy of a computer and conducted a search employing means of a wireless access point while strategically positioned outside 715 West S Street in Lincoln, Nebraska.

Filing No. 15, p. 5.

A defendant moving to suppress evidence on the basis of an alleged unreasonable search must prove he had a legitimate expectation of privacy in the area searched. "Whether a defendant has a constitutionally protected expectation of privacy involves a two-part inquiry—the defendant must show that (1) he has a reasonable expectation of privacy in the areas searched or the items seized, and (2) society is prepared to accept the expectation of privacy as objectively reasonable." Stults, 575 F.3d at 842.

Investigator Weinmaster did not enter the defendant's residence without a warrant, and there is no evidence that he used his laptop and wireless card from the street to enter and obtain records other than those located in defendant's "Shared" computer files.[1] To the

[1]As explained in U.S. v. Lewis, 554 F.3d 208, 211 (1st Cir. 2009):

> When it is first installed, LimeWire creates a folder named "Shared" on the user's computer. By default, any file placed in that "Shared" folder is available to anyone else on the Internet who uses the LimeWire application. Also by default, any file a user downloads through LimeWire is automatically placed in that "Shared" folder and is therefore offered by that user for further downloads by other users. These default behaviors can be changed by the user: a user could turn off sharing altogether, designate another folder with a different name to serve as the "Shared" folder, manually remove files from the "Shared" folder (or whatever folder had been

extent the officer discovered records located on the defendant's computer, the defendant had made those records available to anyone through the installation and use of P2P software. The defendant cannot claim any reasonable expectation of privacy in records he willingly shared with the online world, and he cannot claim his Fourth Amendment rights were violated merely because his P2P sharing audience included a law enforcement officer. United States v. Stults, 575 F.3d 834 (8th Cir.2009) (collecting cases and holding the defendant had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where the defendant had installed LimeWire (a version of P2P software) to make his files accessible to others for file sharing). See also United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008) (where defendant "installed and used file-sharing software on his computer" and "knew or should have known that the folder into which he downloaded files was accessible to others on the peer-to-peer network," that is, "anyone else with the same freely available program," he "lacked an objectively reasonable expectation of privacy in those files," as he thereby "opened up his download folder to the world," and any argument that the defendant "lacked the technical savvy or good sense to configure Lime-Wire to prevent access to his pornography files is like saying that he did not know enough to close his drapes").

The defendant seeks a review under Franks v. Delaware, 438 U.S. 154 (1978), claiming Investigator Weinmaster's description of his wireless access search was intentionally vague, confusing and misleading. Specifically, the defendant claims the officer intentionally or recklessly failed to disclose to the issuing judge that prior to obtaining a warrant, the officer had already viewed the contents of defendant's computer using an unsecured wireless access (referred to by the parties as a "wireless hotspot"). The defendant argues:

---

designated) and prevent them from being shared on an individual basis.

> Although the government claims Weinmaster did not access a computer after conducting the "internet hotspot" search, a common sense construction of his affidavit suggests that he did. If Weinmaster did not conduct such a search, it is impossible to understand why, immediately after saying in his report and his affidavit that he looked for wireless access, he identified the presence of files consistent with child pornography.

Filing No. 20, p. 5. The defendant requests an evidentiary hearing.

Under Franks, a defendant is not entitled to a hearing on his claim that the affiant officer intentionally or recklessly misstated or excluded material information from a warrant application unless he first shows that the warrant application, corrected to remove allegedly false information and to include allegedly concealed facts, would not have supported a finding of probable cause. Franks, 438 U.S. at 170; United States v. Frazier, 280 F.3d 835, 845 (8th Cir. 2002).

> To mandate an evidentiary hearing, the challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine. There must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof. They should point out specifically the portion of the warrant affidavit that is claimed to be false; and they should be accompanied by a statement of supporting reasons. Affidavits or sworn or otherwise reliable statements of witnesses should be furnished, or their absence satisfactorily explained.

Franks, 438 U.S. at 171.

In support of his Franks challenge, the defendant has submitted Investigator Weinmaster's investigation report. The investigation report states:

> On February 1, 2011, I went to the address at 715 West S Street in Lincoln, Nebraska to check on any wireless access points in the area. I parked just west of the residence and used a laptop computer with a wireless card and found eleven wireless access points. Nine of the access points were secured, meaning that you needed the password to log onto the wireless access point. Two of the wireless access points were unsecured, but the signal strengths were very weak from where I was sitting.
>
> As a result of the files that were viewed for sharing from a computer located at this IP address, I viewed four video files that depicted children under the age of eighteen engaged in sexually explicit behavior or conduct along with their SHA1 values that have been [identified] by the automated software as files of child pornography. When I viewed the files that were listed by the automated software for this particular IP address, I proceeded to start the search warrant process. . . .

Filing No. 21-1, at CM/ECF pp. 2-3.

Upon comparing Investigator Weinstein's supplemental investigation report and his warrant application, it is unclear whether the officer used unsecured wireless access to download suspected files, as identified by their names or SHA1 signatures, from the P2P shared file directory of defendant's computer and viewed those downloaded files,[2] or if the officer only identified the suspect files on the defendant's computer by their SHA1 signature, and then actually viewed files with the same SHA1 address available through other online sources and/or from a law enforcement database. The distinction makes no difference.

If the officer viewed actual files residing in the defendant's "Shared" folder and advertised as available for download from defendant's computer, based on the totality of the information within the warrant application, he did so through the use of P2P sharing

[2]The court notes that due to the very weak signal described by the warrant application and the investigator's report, it is unlikely the files themselves were downloaded to the officer's laptop using the unsecured wireless access.

software. The defendant had no reasonable expectation of privacy in these files, and clarifying within the application that the files reviewed by the officer were those actually residing on the defendant's computer would have buttressed, not undermined, the judge's probable cause finding. If the officer did not review files actually downloaded from the defendant's computer, but rather files with the same SHA1 signature as those available for download from IP address 76.84.249.75, the officer reviewed files that were 99.9999 percent certain to be identical to those on the defendant's computer. This level of certainty is substantially more than sufficient to support a finding of probable cause.

There is no evidence Investigator Weinstein "hacked into" any private, "un-shared," areas or folders within the defendant's computer without a warrant, and any argument to the contrary is based on a misunderstanding of how P2P file-sharing works and is intended to work. There is nothing of record to indicate the issuing judge lacked a correct understanding of how P2P sharing software operates. Indeed, it is highly likely Judge Foster fully understood P2P sharing capabilities since the warrant application itself explains those capabilities in great detail; judges receive many such warrant applications outlining information gleaned from P2P shared files; and reported court cases have thoroughly discussed how P2P sharing software is used by suspects and defendants, and thereby becomes useful in law enforcement investigations. See, e.g., U.S. v. Lewis, 554 F.3d 208, 211 (1st Cir. 2009).

The defendant has failed to present any threshold showing that Investigator Weinstein knowingly, intentionally, recklessly (or even negligently) misrepresented or misled the issuing judge. The defendant is not entitled to an evidentiary hearing on his Franks challenge.

For all the foregoing reasons,

IT THEREFORE HEREBY IS RECOMMENDED to the Honorable Richard G. Kopf, United States District Judge, pursuant to 28 U.S.C. § 636(b), that the defendant's motion to suppress, (filing no. 14), be denied in its entirety.

The parties are notified that failing to file an objection to this recommendation as provided in the local rules of this court may be held to be a waiver of any right to appeal the court's adoption of the recommendation.

IT IS FURTHER ORDERED: Trial of this case is set to commence before the Honorable Richard G. Kopf at 9:00 a.m. on September 6, 2011 or as soon thereafter as the case may be called, for a duration of four (4) trial days, in Courtroom 1, United States Courthouse, Lincoln, Nebraska. Jury selection will be held at commencement of trial.

DATED this 5th day of August, 2011.

BY THE COURT:

s/ Cheryl R. Zwart
United States Magistrate Judge

*This opinion may contain hyperlinks to other documents or Web sites. The U.S. District Court for the District of Nebraska does not endorse, recommend, approve, or guarantee any third parties or the services or products they provide on their Web sites. Likewise, the court has no agreements with any of these third parties or their Web sites. The court accepts no responsibility for the availability or functionality of any hyperlink. Thus, the fact that a hyperlink ceases to work or directs the user to some other site does not affect the opinion of the court.